H04K

SECRET COMMUNICATION; JAMMING OF COMMUNICATION

Definition statement

This subclass/group covers:

Two main groups (H04K 1/00 - secret communication, H04K 3/00 - Jamming of communication; Countermeasures), which both relate to communication and to (ensuring or attacking) the security of the physical transmission channel.

H04K 1/00

Secret communication [N: of speech signals] (ciphering or deciphering apparatus per se G09C; systems with reduced bandwidth or suppressed carrier H04B 1/66; spread spectrum techniques in general H04B 1/69; by using a sub-carrier H04B 14/08; by multiplexing H04J; transmission systems for secret digital information H04L 9/00; secret or subscription television systems H04N 7/16)

Definition statement

This subclass/group covers:

Secret communication in the analogue domain for speech and non-speech data.

References relevant to classification in this group

This subclass/group does not cover:

Ciphering or deciphering apparatus per se	G09C
Systems with reduced bandwidth or suppressed carrier	H04B 1/66
Spread spectrum techniques in general	H04B 1/69
By using a sub-carrier	H04B 14/08
By multiplexing	H04J
Transmission systems for secret digital information	H04L 9/00
Secret or subscription television systems	H04N 7/16, H04N 21/00

H04K 3/00

Jamming of communication; Counter-measures (counter-measures used in radar or analogous systems G01S 7/00; [N: in radar G01S 7/36, G01S 7/38; in lidar G01S 7/495; in sonar G01S 7/537])

Definition statement

This subclass/group covers:

- "jamming", only when it means purposefully trying to interfere with the physical transmission and reception of communication.

- provided this condition is met, this group covers devices and methods for:

1. jamming of communication:

1.1 jamming by intentionally decreasing the signal to noise ratio

1.2 deceptive jamming (H04K 3/65)

1.3 passive jamming (H04K 3/68)

1.4 destructive jamming (H04K 3/62)

2. countermeasures against jamming (H04K 3/20 and lower)

3. countermeasures against undesired self-jamming resulting from jamming (H04K 3/28)

4. countermeasures against surveillance, interception or detection (H04K 3/82 and lower)

5. other electronic countermeasures using or against electromagnetic or acoustic waves (H04K 3/00)

6. signal detection techniques used in relation to

6.1. jamming: for interception and monitoring of the jamming target signal (H04K 3/45)

6.2. anti-jamming: for jamming detection (H04K 3/22 and lower)

6.3. anti-surveillance: for surveillance detection (H04K 3/822)

- in particular, this group covers:

1. jamming for testing or assessing countermeasures (H04K 3/94)

2. jamming used to prevent:

- cellular phone communication (H04K 2203/16)

i) in a vehicle during motion (H04K 3/415)

ii) in particular areas, including prisons, hospitals, planes, petrol stations, theatres (H04K 3/84)

iii) to trigger RCIEDs (H04K 3/92 and H04K 2203/24)

- reception of positioning data using GPS (H04K 3/90)

- wireless communication in ad hoc networks or in sensor networks (H04K 2203/18)

- exchange of data between wirelessly connected devices or device units, on Bluetooth, infrared or near field links

- unauthorized access to network, service or information (H04K 3/86), including:

i) access to a WLAN network (H04K 2203/18)

ii) access to information stored in contactless carriers, including RFID carriers (H04K 2203/20)

- transmission of an alarm, against burglary or vehicle theft (H04K 3/88)

- remote control of devices (H04K 3/92)

- surveillance (H04K 3/82 and lower)

i) of speech in meeting rooms (H04K 2203/12)

ii) of electromagnetic emissions from a computer screen H04K 2203/14)

- interception or detection of a wirelessly transmitted signal (H04K 3/825)

Relationship between large subject matter areas

H04K 3/00 and application fields

Application fields (e.g. in the lower part of the "Informative reference" table below): when a patent document discloses how the jamming, anti-jamming, anti-surveillance or any other countermeasure covered by H04K 3/00 is carried out, it should be classified in H04K 3/00.

H04K 3/00 and H04B

Terminology

Jamming should be understood as meaning "intentional disturbance".

Interference should be understood as meaning "unintentional disturbance".

This distinction in the terminology is however not always respected in patent

documents (in particular in the expressions "transceiver self-jamming" and "jamming cancellation", where jamming means interference).

Anti-jamming

Jamming and anti-jamming techniques are covered by H04K 3/00 and lower.

Anti-interference techniques are covered by H04B.

Since intentional and unintentional disturbances often present similar characteristics, they can be countered by the same techniques. Therefore, there exists an overlap between H04K 3/20 and H04B, and some documents are classified in both places.

Cancellation of "self-jamming"

- intentional self-jamming (e.g. self-jamming of receiver to counter interference; self-jamming of transmitter to counter surveillance): H04K;

- undesired self-jamming caused by transmitting: H04B 1/525;

- undesired self-jamming caused by transmitting a jamming signal intentionally: H04B 1/525 and H04K 3/28;

.

H04K 3/00 and H04K 1/00

If the intentional self-jamming signal is known by the transmitter and the receiver of the jammed signal (and can therefore be regarded as a shared secret): H04K 1/00

Other cases of intentional self-jamming: H04K 3/00

References relevant to classification in this group

This subclass/group does not cover:

Counter-measures used in radar	G01S 7/36, G01S 7/38
Counter-measures used in sonar	G01S 7/495
Counter-measures used in lidar	G01S 7/537

Informative references

Attention is drawn to the following places, which may be of interest for search:

Transmission	H04B

Spread spectrum techniques	H04B 1/69 - H04B 1/719
Suppression or limitation of noise or interference	H04B 15/00, H04B 1/10
Reducing, in transceivers, leakage of transmitter signal into the receiver	H04B 1/525
Measuring channel quality parameters	H04B 17/0042
Locating or positioning the transmitter	H04B 17/0072
Gain control	H03G 3/00
Automatic frequency control	H03J 7/00
Shielding	H05K 9/00
Aerials	H01Q
Acoustics	G10K
Electric pulse generators	H03K 3/00
Secret communication	H04K 1/00
Wireless communications networks	H04W
Wireless security	H04W 12/00
Cognitive radio	H04W 16/14, **H04W72/082**
Wireless local area networks (WLAN)	H04W 84/12
Self-organizing networks, ad-hoc networks and sensor networks	H04W 84/18
Handfree telephone for vehicles	H04M 1/6075
Network architectures or network communication protocols for network security for supporting lawful interception, monitoring or retaining of communications or communication related information	H04L 63/30
Flow control or congestion control packet switching networks	H04L 47/135
Television systems	H04N 7/00
Contactless record carriers (e.g. RFID carriers)	G06K 19/00, G06K 7/00
Remote keyless entry	G07C 9/00
Radars and GPS	G01S
Alarm and surveillance	G08B

Vehicle anti-theft relating to remote keyless entry	B60R 25/00
Vehicle anti-theft alarm transmission	B60R 25/102
Weapons	F41
Defence devices	F41H 11/00

Special rules of classification within this group

A patent document should be classified in H04K 3/20 when the countered signal disturbance is:

- intentional (whether offensive or defensive) or

- used in a military, security or confidentiality context.

Glossary of terms

In this subclass/group, the following terms (or expressions) are used with the meaning indicated:

Jamming of communication	Purposefully trying to interfere with the physical transmission or reception of communication
Self-jamming resulting from jamming	Undesired interference, caused by a jamming device, to the communication of the jamming device itself or of a friendly device, and resulting from intentionally interfering with the communication of adversary devices
Follower jammer	Jammer adapted to determine and follow the frequency of a jamming target signal that uses frequency hopping techniques
Look-through mode	Operation mode wherein jamming and monitoring of the jamming target alternate
Reactive jammer	Jammer wherein jamming is activated only when a target has been detected

Synonyms and Keywords

In patent documents the following abbreviations are often used:

(F)FH	(Fast) Frequency Hopping
GPS	Global Positioning System
NFC	Near Field Communication

RCIED	Remote Controlled Improvised Explosive Device
RFID	Radio Frequency IDentification
WLAN	Wireless Local Area Network